Amendment

(Amendment under the provisions of Article 11 of PCT)

PCT 09,2,04 (Reception Seal)

To: Director General, Patent Office

1. Designation of International Application: PCT/JP03/07794

2. Applicant:

Name: ADVANCED COMPUTER SYSTEMS, INC.

Address: 915-15, Shinmaruko-machi, Nakahara-ku, Kawasaki-shi, Kanagawa 211-0005 Japan

Nationality: JAPAN

Residence: JAPAN

3. Proxy:

Name: 8151 Patent Attorney; SAKAI Hajime

Address: Shuwa Kioicho TBR Building, 7, Kojimachi 5-chome, Chiyoda-ku, Tokyo 102-0083 Japan

4. Object of Amendment: Specification and Claims

5. Content of Amendment:

(1) Description of "$B_m = w(C, Q) = C_{m-1} + Q_{m-1}$" in line 13 on page 37 (line 18 on page 58 in English text) of the specification is amended to -- $S_m = z(C, Q) = C_m + Q_{m-1}$ --.

(2) Description of "according to claim, wherein," in line 3 of Claim 27 on page 81 (page 128 in English text) of the Claims is amended to -- according to claim 25, wherein, --.

6. List of Attached Documents:

(1) Page 37 of the specification

(2) Page 81 of Claims

Here, m is a natural number and $m \geq 1$.

The secret data *C* on the client computer 10 side and the secret data *S* of on the server computer 40 side are transmitted to the other, and as explained in the following, the secret data changes every time of information giving/receiving. In other words, as to the secret data *C* transmitted from the client computer 10 to the server computer 40, at the transmission timing above, new secret data *C* is generated by a predefined function $y(S, R)$, and then it is transmitted. The function *y* may be a simple addition, polynomial equation with a coefficient added, multiplication, sum of products and hash function, as a way of example. Similarly, when a transmission is made from the server computer 40 to the client computer 10, the secret data *S* is generated by a predefined function $z(C, Q)$ and it is transmitted. The function *z* may be a simple addition, polynomial equation with a coefficient added, multiplication, sum of products and hash function, as a way of example. An example of the function *y* and the function *z* will be shown in the following.

$$C_m = y(S, R) = S_{m-1} + R_{m-1}$$

$$S_m = z(C, Q) = C_m + Q_{m-1}$$

Here, m is a natural number and $m \geq 1$.

In addition, it may be possible to conceal the secret data

transmission, in order to make difficult for a third party to specify the secret data. For example, the secret data C transmitted from the client computer 10 to the server computer 40 and the secret data S transmitted from the server computer 40 to the client computer 10 may be concealed by the private key K. In other words, it is possible to use a function to which the private key K is added as a parameter.

(Detailed process)

Fig. 4 is a conceptual illustration showing a detailed process in the mutual authentication according to the first embodiment of the present invention. The detailed process of the present embodiment will be explained with reference to Fig. 4.

Step P0:

In each of the client computer 10 and the server computer 40, a private key K_0 as initial value is stored. This process corresponds to step 100 of Fig. 3, and processes Pc0 and Ps0 of Fig. 4.

Step P1:

In the client computer 10, a random number R is generated, secret data C and authentication data A are computed and transmitted to the server computer 40.

a step in which said first device generates, as the third onetime ID, a function value of one-way function in which said first random number, said second random number, and said shared key are used as arguments, and transmits the third onetime ID to said second device; and

a step in which said second device generates by computation said third onetime ID based on said first random number, said second random number and said shared key, and determines validity of said first device by comparing a result of the computation and said third onetime ID received from said first device.

26. The authentication method according to claim 24, wherein,

said first random number and said second random number are transmitted in a state as being encrypted by a shared key previously shared between said first device and said second device.

27. The authentication method according to claim 25, wherein,

said first random number and said second random number are transmitted in a state as being encrypted by a shared key previously shared between said first device and said second device.

28. The authentication method according to any one of claims 24 to 26, wherein,

in the step where said second device transmits to said first device said second onetime ID and said second random number, said second device has, as an initial random number, a random number shared between the second device and said first device, and carries out a predefined computation in which the initial random number and said first random number are used as arguments, and transmits a result of the computation to said first device, and said first device uses said result of the computation received from said second device as a material for determining validity of said second device, together with said second onetime ID.

29. The authentication method according to claim 24, wherein,

in the step where said first device transmits said third onetime ID to said second device, said first device carries out a predefined computation in which said first random number and said second random number are used as arguments, and transmits a result of the computation to said second device, and said second device uses said result of the computation received from said first device as a material for determining validity of said first device, together with said third onetime ID.

30. The authentication method according to claim 25, wherein,

in the step where said first device transmits said third onetime ID to said second device, said first device carries out a predefined computation in which said first random number and said second random number are used as arguments,